Testimony of Adam H. Greene, JD, MPH
Partner, Davis Wright Tremaine LLP
National Committee on Vital & Health Statistics
Subcommittee on Privacy, Confidentiality & Security

"Minimum Necessary and the Health Insurance Portability and Accountability Act (HIPAA)"

June 16, 2016

Capital Hilton Hotel
1001 16th Street, NW, Federal A Room
Washington, DC 20036

Good morning and thank you for this opportunity to provide testimony to the Subcommittee on this important topic. My name is Adam Greene, and I am a partner in the law firm of Davis Wright Tremaine and co-chair of its health information practice. My practice generally focuses on health information privacy and security, and in particular HIPAA. My clients include health care providers, health plans, and a wide range of business associates. Prior to joining DWT, I was with the U.S. Department of Health and Human Services for five years working on HIPAA-related issues, first within the Office of General Counsel and later within the Office for Civil Rights.

In the abstract, HIPAA's minimum necessary standard makes complete sense. Only members of the workforce who need to use protected health information for their job function should have access to such information. The amount of protected health information to which they have access should be appropriately limited. Entities should only disclose the amount of protected health information that is necessary for the objective of the disclosure, and likewise should only request the amount of protected health information that is necessary. Requesting or disclosing the full medical record should be a last resort that requires particular justification. It is hard to argue with any of these principles.

But sometimes good policies conflict with practical realities. In my transition from government to private practice, it quickly became apparent that these laudable goals become a lot more complicated in the real world. For my testimony, I would like to focus on three particular challenges and areas of ambiguity with current policies: (1) the application of the minimum necessary standard in electronic health information exchange; (2) the challenges for business associates under existing guidance; and (3) the burden versus the benefit of the minimum necessary implementation specifications for routine requests and disclosures.

1. Electronic Health Information Exchange

Electronic health information exchange, in its many forms, presents incredible opportunities to transform the health care system for the better. Much of this opportunity involves improving treatment, such as making it easier for physicians to exchange patient information with each other or to pull a patient's medical history in an emergency situation. These uses are easy with respect to the minimum necessary standard, as the regulations exempt treatment requests, uses, and disclosures from the minimum necessary requirements.

But improving individualized treatment is not the only potential benefit of health information exchange. It also provides opportunities to improve the quality of care and to reduce costs, which generally are treated as "health care operations" under HIPAA. It can also improve the ability of health care providers and health plans to interact for payment-related activities, including moving payment systems towards more value-based programs. Unlike treatment activities, these types of activities are subject to HIPAA's minimum necessary standards. And it is in these areas that the minimum necessary standard becomes very problematic.

The fundamental problem is that health information exchange currently operates by providing complete access to an electronic medical record or by providing a particular subset of information. My impression is that there generally is not a means to limit the request or the provision of access to that which is the minimum necessary amount. This means that entities generally will be requesting or disclosing either more or less than that which is necessary. Doing so raises concerns of noncompliance with the minimum necessary standards.

For example, if a health plan wants to utilize health information exchange to determine whether a patient's power wheelchair is medically necessary, it likely cannot request access to only information related to the condition that necessitates the wheelchair. And, likewise, the health care provider or health information exchange organization likely cannot limit access to only the most relevant information. Instead, depending on the structure of the health information exchange, the health care provider or health information exchange organization may need to provide access to the entire medical record, or to a standardized subset of information that potentially includes too much or too little medical information.

This puts all parties involved in health information exchange at legal risk. The health plan is at risk for having requested too much information in violation of the minimum necessary standard. The health care provider or health information exchange organization is at risk of having disclosed too much information (as "disclosure" includes any "provision of access" to information). Accordingly, organizations are left with a choice. They can proceed with health information exchange efforts that are focused on improving health care operations and payment activities and accept a significant legal risk that they will be found in violation of HIPAA. Or they can limit their health information exchange activities to treatment (and disclosures pursuant to authorizations), foregoing potentially beneficial activities that may reduce costs of health care or improve quality of care.

Now, as much as I am a technology optimist, I am skeptical that there are technical solutions to this problem. I don't envision health information exchange readily reaching a point where each request and provision of access can reasonably be limited to only the information that is needed.

Instead, I think that the solution to this problem lies in changes to policy or guidance. For example, it would be helpful to revise the regulations or issue guidance that, with respect to electronic access, a covered entity only violates the minimum necessary standard if it actually accesses more protected health information than is necessary. In contrast, providing access to the entire medical would not be a violation where the other party has a permissible reason to access some portion of some medical records. This would be a departure from the existing minimum necessary provisions' focus on requests and disclosures, but it would allow greater variety of health information exchange while still leaving in place mechanisms to ensure that there are limits on how much information is actually accessed.

2. Business Associates

Current guidance provides:

> A covered entity's contract with a business associate may not authorize the business associate to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. See 45 CFR 164.504(e)(2)(i). Thus, a business associate contract must limit the business associate's uses and disclosures of, as well as requests for, protected health information to be consistent with the covered entity's minimum necessary policies and procedures.

http://www.hhs.gov/hipaa/for-professionals/faq/252/may-covered-entity-rely-on-a-request-from-a-business-associate/index.html. This guidance dates back to 2002, and was reiterated in the HIPAA Omnibus Rule's preamble commentary in 2013.

The problem with this guidance is that there are some organizations that are business associates to thousands, or even tens of thousands of covered entities. If each covered entity adopted its own set of minimum necessary policies and procedures, no business associate can realistically comply with each unique set of policies and procedures.

This is not the only supportable interpretation of the regulations. Instead, each business associate should be responsible for independently complying with the minimum necessary standard, the same way a covered entity must do so. This is consistent with most other HIPAA provisions. For example, with respect to every Security Rule provision, a business associate is expected to independently comply with the Security Rule requirement, potentially implementing the requirement differently than the covered entity based on the business associate's unique environment.

Such an interpretation would not reduce the requirement for business associates to comply with the minimum necessary standard. Rather, it would acknowledge the practical reality that no business associate should be expected to comply with someone else's policies, and certainly cannot be expected to comply with thousands of other entities' policies.

3. Burden of Current Minimum Necessary Implementation Specifications

Section 164.514(d) of the HIPAA regulations include a number of implementation specifications for the minimum necessary standard. For example, the regulations provide that "[f]or any type of disclosure that it makes on a routine and recurring basis, a covered entity must

implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure." Similarly, "[f]or a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made."

Health care providers and health plans are complex organizations, continuously making a wide range of disclosures and requests for protected health information. To try to create minimum necessary protocols for every such routine disclosure or request is a herculean task. And I believe that the burden of doing so far outweighs any benefit. The minimum necessary standard should still apply, but it need not lead to drowning in a sea of "standard protocols." I cannot think of another provision of the HIPAA regulations that calls for such voluminous documentation. Rather, there are far better places to focus health care organization's resources. Accordingly, I suggest that it is time to reconsider the idea of documenting minimum necessary protocols for every type of recurring disclosure or request, as the burden of such a system far outweighs any corresponding benefit to patients.

* * * * *

Make no mistake, the minimum necessary standard is one of the most important parts of the Privacy Rule, and the principles underlying it are as important today as they were over 15 years ago. But we have gained a lot of experience witnessing what works and what does not, and we have seen exciting technological changes that were not envisioned when the Privacy Rule was first drafted. Accordingly, it is an opportune time to revisit these regulatory provisions and improve upon them.

Thank you for your consideration of these issues. I look forward to answering any questions you might have.